How Can Botnets Cause Storms? Understanding the Evolution and Impact of Mobile Botnets

Zhuo Lu[†], Wenye Wang[†], and Cliff Wang[‡]

[†] Department of Electrical and Computer Engineering
North Carolina State University, Raleigh NC, US.

[‡] Army Research Office
Research Triangle Park NC, US.

Apr., 2014

Outline

1. Motivation
   - Mobile Applications, Malware and Botnets
   - Research Issues and Our Focus
2. Preliminaries
   - Network and Attack Models
   - Problem Formulation
3. Results
   - Botnet Propagation
   - Mobile Botnet Impact
4. Conclusion

Outline

1 Motivation
- Mobile Applications, Malware and Botnets
- Research Issues and Our Focus

2 Preliminaries

3 Results

4 Conclusion

Smart Phone, Mobile Malware, and Mobile Botnet

Smart Phones

- Powerful hardware, mobile operating systems, mobile APPs.
- Mobile malware has come into practice.

Smart Phone, Mobile Malware, and Mobile Botnet

Smart Phones

- Powerful hardware, mobile operating systems, mobile APPs.
- Mobile malware has come into practice.

The Threat of Mobile Botnets

Mobile botnet: A collection of malware infected nodes able to perform coordinated attacks.

- Ikee.B in 2009
- Android.Bmaster in 2011.

Smart Phone, Mobile Malware, and Mobile Botnet

Smart Phones

- Powerful hardware, mobile operating systems, mobile APPs.
- Mobile malware has come into practice.

The Threat of Mobile Botnets

Mobile botnet: A collection of malware infected nodes able to perform coordinated attacks.

- Ikee.B in 2009
- Android.Bmaster in 2011.
- [Traynor '09]: a botnet with sufficiently many infected phones is able to disrupt regional cellular services.

How Mobile Botnets Propagate in the Network

The ways that a botnet propagates in mobile networks

- Centralized propagation: SMS/MMS, APPs in the market.
  - Becoming harder and harder.

How Mobile Botnets Propagate in the Network

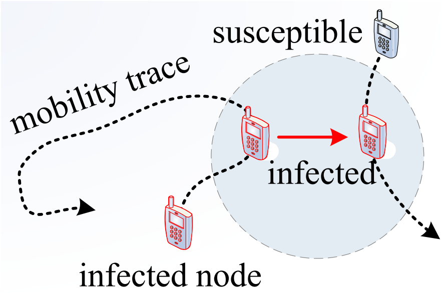
The ways that a botnet propagates in mobile networks

- Centralized propagation: SMS/MMS, APPs in the market.
    - Becoming harder and harder.
- Mobile-to-mobile/Proximity infection: More stealthy!

How Mobile Botnets Propagate in the Network

The ways that a botnet propagates in mobile networks

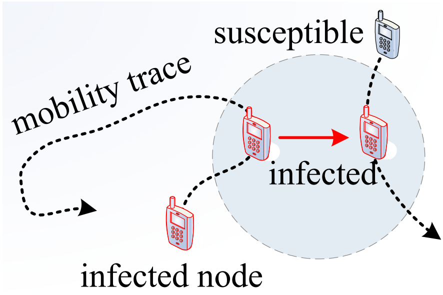
- Centralized propagation: SMS/MMS, APPs in the market.
    - Becoming harder and harder.
- Mobile-to-mobile/Proximity infection: More stealthy!



How Mobile Botnets Propagate in the Network

The ways that a botnet propagates in mobile networks

- Centralized propagation: SMS/MMS, APPs in the market.
  - Becoming harder and harder.
- Mobile-to-mobile/Proximity infection: More stealthy!

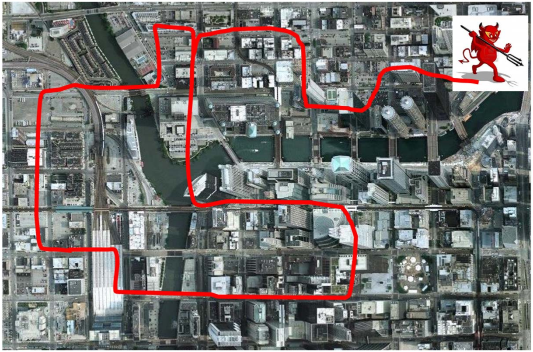


- Existing malware adopting proximity infection.
  - E.g., Mabir, Lansco and CPMC.

Research Question and Issues in the Literature

Question?

Can Mobile Malware via Proximity Infection Cause Storms?



Research Question and Issues in the Literature

Question?

Can Mobile Malware via Proximity Infection Cause Storms?

Answers

- Yes ([Carettoni'07, Yan'09, Wang'09]): Epidemic modeling and experiments
  - Infection storm: More and more nodes get infected as time goes.
- No ([Husted'11]): Simulations in realistic mobile scenarios.
  - Limited infection: the number of infected devices is limited with the relatively low vulnerability ratio.

Research Question and Issues in the Literature

Question?

Can Mobile Malware via Proximity Infection Cause Storms?

Answers

- Yes ([Carettoni'07, Yan'09, Wang'09]): Epidemic modeling and experiments
  - Infection storm: More and more nodes get infected as time goes.
- No ([Husted'11]): Simulations in realistic mobile scenarios.
  - Limited infection: the number of infected devices is limited with the relatively low vulnerability ratio.

Somewhat discrepant results in the literature.

- Why: Node density, mobility, vulnerability ratio?

Research Question and Objective

Research Question

How to model the botnet propagation and impact in mobile networks?

Research Question and Objective

Research Question

How to model the botnet propagation and impact in mobile networks?

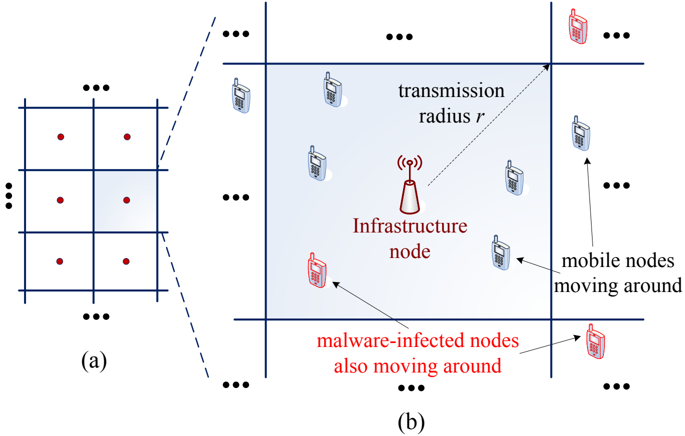
Objectives

1. Characterize how fast a mobile botnet propagates.
2. Investigate the denial-of-service impact of such a botnet.

Outline

Network Model

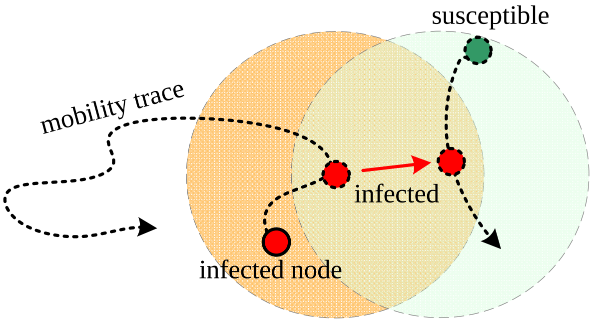
A hybrid network: infrastructure and mobile nodes.



transmission range r, mobile node density λ, network bandwidth B

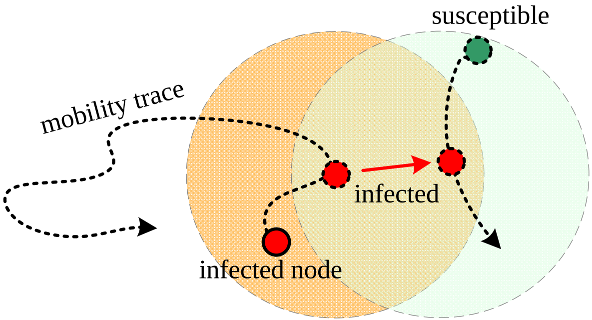
Propagation Model: Proximity Infection

How to propagate malware from one node to another?



Propagation Model: Proximity Infection

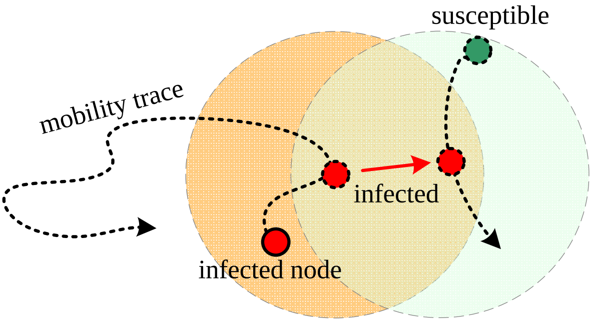
How to propagate malware from one node to another?



1. One is infected, another is vulnerable (vulnerability ratio κ).

Propagation Model: Proximity Infection

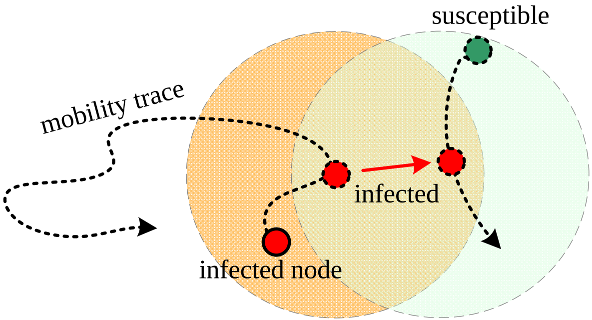
How to propagate malware from one node to another?



1. One is infected, another is vulnerable (vulnerability ratio κ).
2. Two nodes are in each other's transmission range (r).

Propagation Model: Proximity Infection

How to propagate malware from one node to another?



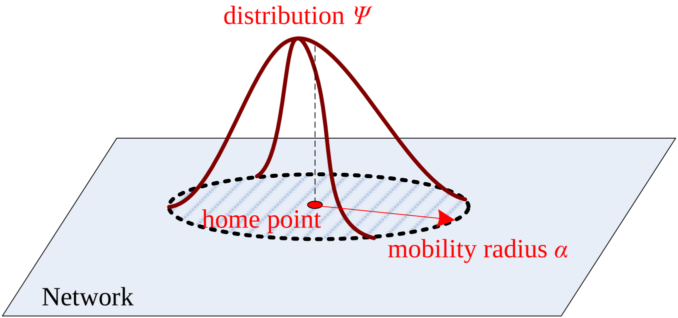
1. One is infected, another is vulnerable (vulnerability ratio κ).
2. Two nodes are in each other's transmission range (r).
3. Meeting time $>$ threshold.

Mobility Model: Generic Mobility

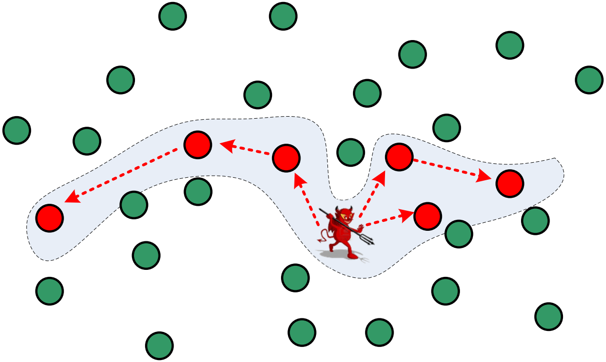
Realistic mobility always incurs spatial heterogeneity.

Mobility Model: Generic Mobility

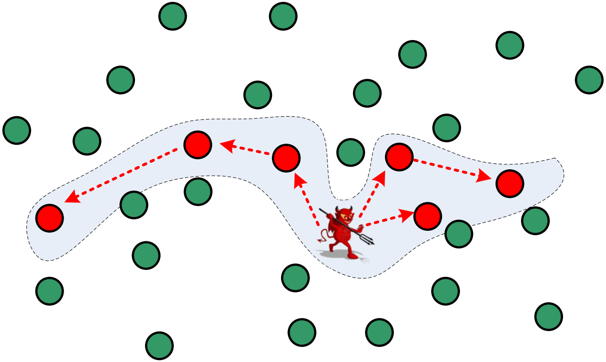
Realistic mobility always incurs spatial heterogeneity.



Problem Formulation and Performance Metric

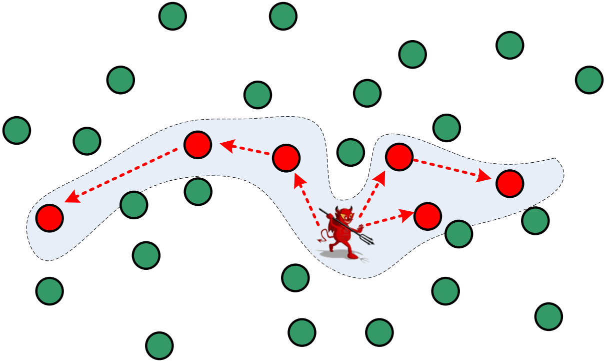


Problem Formulation and Performance Metric



- Botnet $\mathcal{S}(t)$: the set of all infected nodes at t.

Problem Formulation and Performance Metric



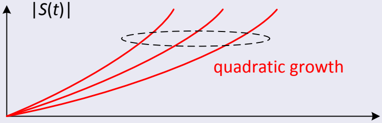
- Botnet $\mathcal{S}(t)$: the set of all infected nodes at t.
- Question: What is the botnet size $|\mathcal{S}(t)|$ at time t?

Outline

Theoretical Results

Theorem: Mobile Botnet Propagation

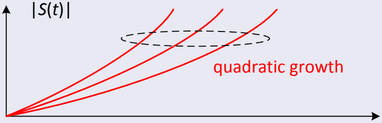
If the value of $\kappa\lambda(2\alpha + r)$ is sufficiently large, we have a botnet propagation storm: the average botnet size $\mathbb{E}|\mathcal{S}(t)| = \Theta(t^2)$.



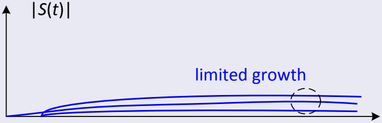
Theoretical Results

Theorem: Mobile Botnet Propagation

If the value of $\kappa\lambda(2\alpha + r)$ is sufficiently large, we have a botnet propagation storm: the average botnet size $\mathbb{E}|\mathcal{S}(t)| = \Theta(t^2)$.



Otherwise, we have limited propagation: $\mathbb{E}|\mathcal{S}(t)| = \Theta(1)$.



Theoretical Results

Theorem: Mobile Botnet Propagation

If the value of $\kappa\lambda(2\alpha + r)$ is sufficiently large, we have a botnet propagation storm: the average botnet size $\mathbb{E}|\mathcal{S}(t)| = \Theta(t^2)$. Otherwise, we have limited propagation: $\mathbb{E}|\mathcal{S}(t)| = \Theta(1)$.

Direct Indications

1. Fastest rate of proximity infection: quadratic growth.
   - Internet botnets: exponential growth.

Theoretical Results

Theorem: Mobile Botnet Propagation

If the value of $\kappa\lambda(2\alpha + r)$ is sufficiently large, we have a botnet propagation storm: the average botnet size $\mathbb{E}|\mathcal{S}(t)| = \Theta(t^2)$. Otherwise, we have limited propagation: $\mathbb{E}|\mathcal{S}(t)| = \Theta(1)$.

Direct Indications

1. Fastest rate of proximity infection: quadratic growth.
   - Internet botnets: exponential growth.
2. $\kappa\lambda(2\alpha + r)$ is the key
   - density λ, mobility radius α, transmission range r.

Theoretical Results

Theorem: Mobile Botnet Propagation

If the value of $\kappa\lambda(2\alpha + r)$ is sufficiently large, we have a botnet propagation storm: the average botnet size $\mathbb{E}|\mathcal{S}(t)| = \Theta(t^2)$. Otherwise, we have limited propagation: $\mathbb{E}|\mathcal{S}(t)| = \Theta(1)$.

Direct Indications

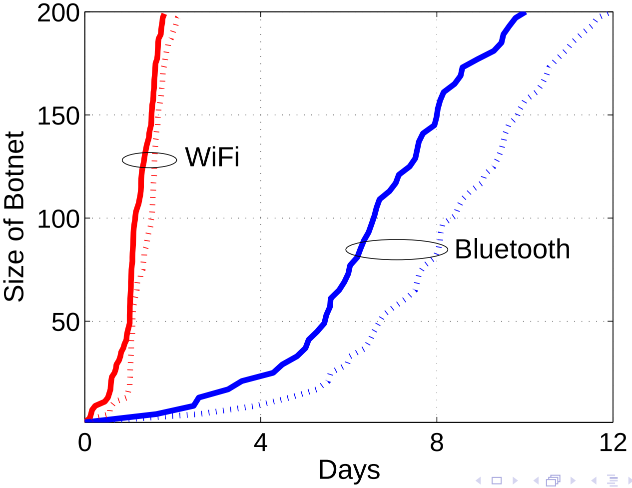
1. Fastest rate of proximity infection: quadratic growth.
   - Internet botnets: exponential growth.
2. $\kappa\lambda(2\alpha + r)$ is the key
   - density λ, mobility radius α, transmission range r.
   - Practical scenario: density λ and transmission range r fixed
   - Sufficient mobility always triggers the $\Theta(t^2)$ infection!

Experimental Evaluation: Setups

- Mobility traces: EPFL/mobility data set: 300 cabs in San Francisco.

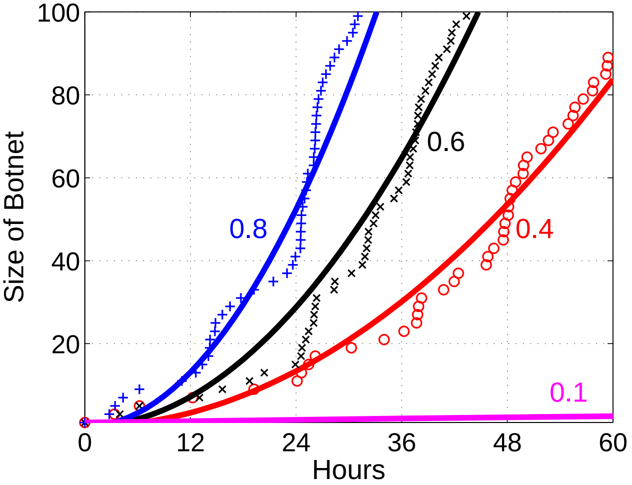
- Initially infected node: one cab is randomly chosen.
- Running period: 12 days.
- Wireless transmission range: Bluetooth (10m), WiFi (100m)
- Vulnerability ratio: 10% - 80%

The size of botnet with two different initially infected nodes and $\kappa = 80\%$.



Experimental Evaluation: Results

The size of botnet with different vulnerability ratios κ and WiFi.



Summary: EPFL Data Set

For different setups, we always observe the quadratical increase of the botnet size!

- Different vulnerability ratios
- Different transmission ranges
- Different initially infected nodes

Summary: EPFL Data Set

For different setups, we always observe the quadratical increase of the botnet size!

- Different vulnerability ratios
- Different transmission ranges
- Different initially infected nodes

Reason: Cab movements during 12 Days

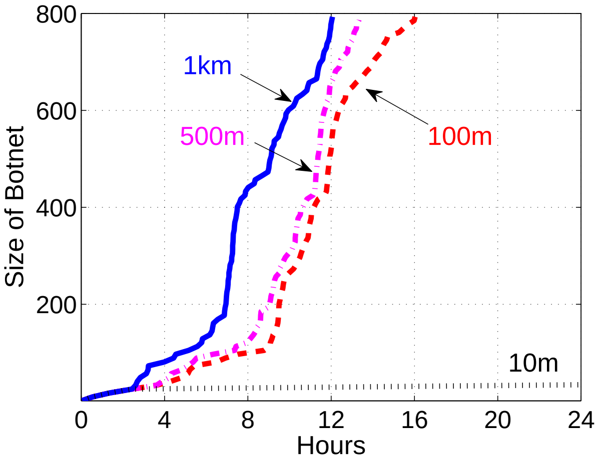
- sufficient mobility in San Francisco area.
- mobility radius α is large.

Experiments with Limited Mobility

- UDelModels: a tool to generate realistic mobility traces.
- Map: 2000 nodes in 2km×2km downtown Chicago, κ=60%, r = 10m (bluetooth),
- Mobility radius α=10, 100, 500, 1000m.

Experimental Results

The botnet size with different mobility radius α.



The Impact of Botnet Attacks

Quadratic growth: A botnet can become larger and larger

- Launching attacks targeting a mobile service. [Traynor '09]
- Infected nodes flood service requests.

The Impact of Botnet Attacks

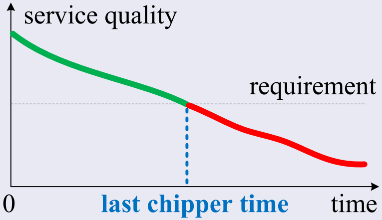
Quadratic growth: A botnet can become larger and larger

- Launching attacks targeting a mobile service. [Traynor '09]
- Infected nodes flood service requests.

Question: If a botnet starts to propagate at time 0, how long the botnet is able to launch an attack to take down a service?

The Impact of Botnet Attacks

Performance Metric: Last Chipper Time

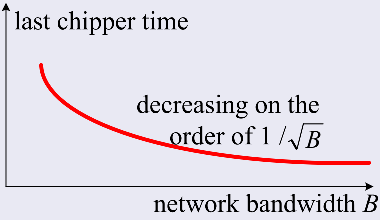


The last time that a required ratio ($\sigma < 1$) of mobile service requests can still be processed on time under the botnet attack,

$$T_l = \sup\{t \geq 0 : \mathbb{P}(D_p < d) > \sigma\}.$$

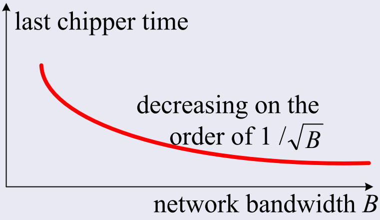
The Impact of Botnet Attacks

Theorem: Last chipper time decreases on the order of $1/\sqrt{B}$



The Impact of Botnet Attacks

Theorem: Last chipper time decreases on the order of $1/\sqrt{B}$

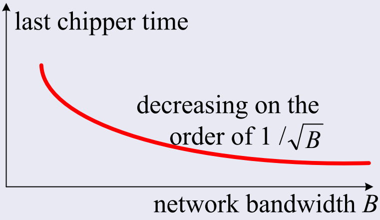


Increasing network bandwidth:

- improves network performance
- a botnet can propagate for a shorter time to disrupt a service.
    - less time to detect and respond the attack!

The Impact of Botnet Attacks

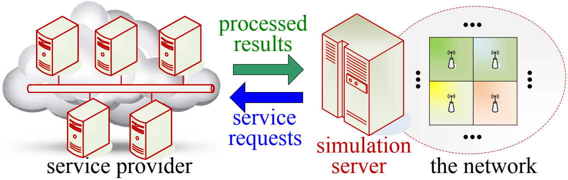
Theorem: Last chipper time decreases on the order of $1/\sqrt{B}$



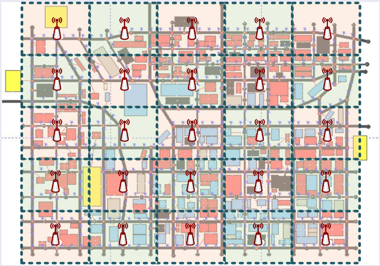
Example: LTE→LTE Advanced (10 times bandwidth increase).
Last chipper time becomes $1/\sqrt{10} \approx 1/3$ of the time in LTE.

Experimental Evaluation

Experimental setups

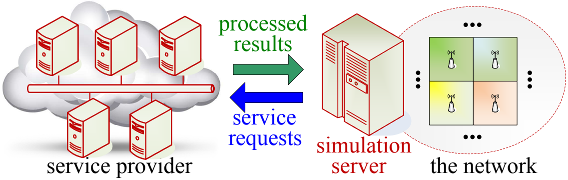


The Network: 2km$\times$2km downtown Chicago, 25 APs



Experimental Evaluation

Experimental setups

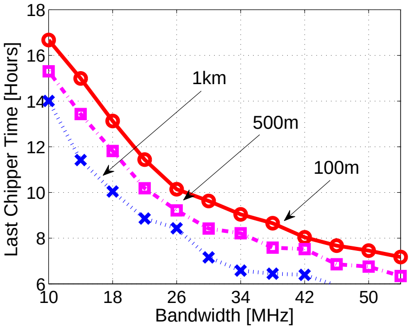


Service provider: small-scale

- 7 computers over Storm framework (real-time distributed processing).
- Service quality requirement: 90% on time.
- Service timing requirement: 2 seconds.

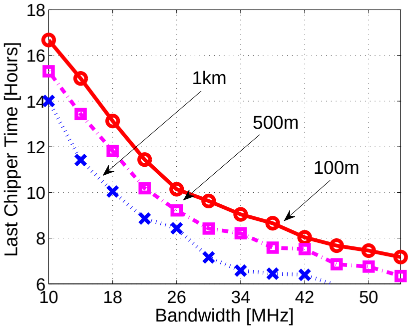
Experimental Results

The last chipper time with different mobility radius, κ=60%.



Experimental Results

The last chipper time with different mobility radius, κ=60%.



- Last chipper time decreases on the order of $1/\sqrt{B}$
- Increasing B increases the risk of service being disrupted.

Outline

Conclusion

1. We investigated how mobile botnets evolve via proximity infection and their impacts.

2. We found mobility can be a key to the size of a mobile botnet.
   - Sufficient mobility → the size increases quadratically over time.
   - Insufficient mobility → the size is bounded by a constant.

3. We defined the metric of last chipper time that offers quantitative risk assessment on potential denial-of-service impacts of botnet attacks in mobile networks.

Thank you!